REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-04-2008	FINAL	

4. TITLE AND SUBTITLE

Military Deception and the Non-State Actor

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

James K. Hansen

Paper Advisor: Gary Reed-Chambers

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

United States military joint doctrine was designed with a conventional enemy in mind. However, as the United States finds itself embroiled in more and more unconventional conflicts an assessment regarding the applicability of current joint doctrine needs to be conducted. This paper discusses the joint doctrine of Military Deception and its applicability against a non-state actor. It looks at the basic tenets of military deception doctrine, conventional historical examples, organizational structures utilized by non-state actors, and an unconventional historical example. The paper then provides some guidance to the operational commander on how to best evaluate the adversarial decision maker and identify potential channels of influence through which a successful deception operation can be conducted. Finally, the paper concludes with an opinion on the applicability of current joint military deception doctrine against a non-state actor and recommendations on how an operational commander can best be prepared for success against his unconventional adversary.

15. SUBJECT TERMS

Military Deception, Non-State Actor, Terrorism, Insurgency, Maskirovka

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Military Deception and the Non-State Actor

by

James K. Hansen

LCDR, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

23 April 2008

Table of Contents

List of Illustrations

Abstract

United States military joint doctrine was designed with a conventional enemy in mind. However, as the United States finds itself embroiled in more and more unconventional conflicts an assessment regarding the applicability of current joint doctrine needs to be conducted. This paper discusses the joint doctrine of Military Deception and its applicability against a non-state actor. It looks at the basic tenets of military deception doctrine, conventional historical examples, organizational structures utilized by non-state actors, and an unconventional historical example. The paper then provides some guidance to the operational commander on how to best evaluate the adversarial decision maker and identify potential channels of influence through which a successful deception operation can be conducted. Finally, the paper concludes with an opinion on the applicability of current joint military deception doctrine against a non-state actor and recommendations on how an operational commander can best be prepared for success against his unconventional adversary.

INTRODUCTION

Since the beginning of recorded history, military deception has been used by military forces seeking advantage over their enemy. History is replete with military strategists discussing the importance of deception in war. Writing in the sixth century B.C., Sun Tzu captured the importance of deception when he wrote "All warfare is based on deception" and went on to explain that, "…when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[1] Mao Tse-Tung, writing twenty-five centuries later on guerrilla warfare, stated that a guerrilla force must "…select the tactic of seeming to come from the east and attacking from the west; avoid the solid, attack the hollow; attack; withdraw; deliver a lightning blow, seek a lightning decision."[2] Today, the importance of military deception has not been forgotten and even has its own U.S. military joint publication. However, while the theory of deception has been widely accepted as useful over the centuries, moving from theory into practical application has been and remains the most challenging aspect of military deception operations. Making this challenge even greater for today's operational commander is the fact that he is more likely to encounter an insurgency force, terrorist group, or other non-state actor than he is traditional military force of an enemy state. So the question arises, can the operational commander effectively use military deception against a non-state actor? This paper will show that while combating a non-state actor provides challenges not associated with a traditional enemy force, the principles of military deception can still be applied.

DOCTRINE

According to current U.S. military joint doctrine, military deception is one of the major elements that can be leveraged to wage a successful Information Operation campaign or operation and is defined as "… those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[3] At the operational level, military deception is described as influencing "…the decisions of adversary commanders before, during, and after battle so the tactical outcome can be exploited at the operational level."[4] It is important to look at these definitions more closely to discover what adversary the drafters of the doctrine had in mind when they wrote it. The first definition addresses the "adversary decision makers" and does not specify that these decision makers are the leadership of an opposing enemy military force.[5] This allows the definition to be interpreted as enabling military deception to be applied to any type of adversary that the military is sent to engage, including terrorists, insurgency groups, or even the possibility of criminal organizations. The operational definition, however, goes on to use the military terms "commander" and "battle" to describe who is being targeted and the objective of deception. This does not necessarily tie the doctrine to a military engagement but it does demonstrate that at the operational level at least, a deception operation is most likely intended to be used during military-on-military engagements. However, what is most telling about the definition of military deception is that the only way it has changed since 1996 is the substitution of the word "military" with the word "adversary".[6] Additionally, there was no separate definition for operational military deception, so a new one was added.[7] The word substitution and further clarification on what

constitutes military deception at the operational level demonstrates intent by the Department of Defense (DoD) to widen the applicability of military deception operations, but I would argue that these simple changes do not improve the operational commander's ability to adapt what was exclusively military specific doctrine to a doctrine that deals effectively with the non-state actor. It is still incumbent upon the operational commander to adapt a conventionally focused doctrine to an unconventional situation.

When conducting military deception operations, the operational commander has three primary means of deception at his disposal: physical, technical, and administrative.[8] Physical means of deception include operational activities and resources such as movement of forces, the use of decoy equipment, tactical actions, and reconnaissance and surveillance.[9] Technical means of deception can be used to either deny or convey information to the adversary. Some of the technical means include the emissions of radar signals, radio transmissions, biological odors, and use of the internet.[10] The final means of deception is administrative and includes the use of military orders, messages, papers, or pictures that may be useful in conveying the deceptive message to the adversary.[11] These administrative items may be real or forged, depending on the objective or objectives of the deception operation. These means of deception can easily be applied to actions against both a traditional military force and other types of enemy force. It is incumbent upon the operational commander and his planning staff to adjust the means to those capabilities of their adversary. For example, false radar emissions are unlikely to be detected by a terrorist organization's intelligence arm due to technological limitations and therefore will never be passed to the adversary decision makers to influence their decisions. On the other hand, papers and unsecured radio emissions

are more easily intercepted and could easily find their way into the adversary's decision making process.

As previously mentioned, the goal of any military deception operation is to mislead the adversary decision maker, but of what are we trying to convince them? Joint Publication 3-13.4 lists nine possible objectives of a military deception operation. They are:

1. Mask an increase in or redeployment of forces or weapons systems spotted by the adversary.
2. Shape the adversary's perception and/or identification of new forces or weapons being introduced into combat.
3. Reinforce the adversary's preconceived beliefs.
4. Distract the adversary's attention from other activities
5. Overload adversary ISR collection and analytical capabilities.
6. Create the illusion of strength where weakness exists.
7. Desensitize the adversary to particular patterns of friendly behavior to induce adversary perceptions that are exploitable at the time of friendly choosing.
8. Confuse adversary expectations about friendly size, activity, location, unit, time, equipment, intent, and/or style of mission execution, to effect surprise in these areas.
9. Reduce the adversary's ability to clearly perceive and manage the battle.[12]

By no means are these nine objectives all inclusive, but they are representative of what has been the preponderance of deception objectives in the past. Since we already know that our military deception doctrine was designed for a conventional enemy military force, do these objectives retain their relevancy against the non-state actor? As long as the military commander has been able to accurately identify who constitutes the adversary force, especially its intelligence gathering cell, in theory there is no reason that these objectives cannot be met. As I will discuss later in the paper, unfortunately for the operational commander, identifying who is involved in the non-state actor organization can be a difficult task.

The last doctrinal aspect of military deception that concerns the commander's execution of an operation is the four main deception techniques: feints, demonstrations,

ruses, and displays.[13] Feints are offensive actions utilized to misdirect the adversary as to the time and/or place of the true operation.[14] Demonstrations are a show of force that is intended to misdirect the adversary's consolidation of forces.[15] Ruses are the intentional exposure of information to the adversary with the intent of misdirection.[16] Lastly, displays utilize many of the physical means of deception to portray misleading types or numbers of forces to the adversary's intelligence assets.[17] It is by utilizing these techniques, which contain the means of deception, that the military commander can obtain his objectives. As with the objectives doctrine discussion, theoretically there is no reason that these four deception techniques cannot be used on any type of adversary, but their effectiveness is dependent upon the operational commander's level of understanding as to how his adversary is organized, operates, and makes its operational decisions.

CONVENTIONAL HISTORICAL CASES

Now that I have discussed the basic tenants of military deception doctrine, it will be beneficial for the reader to have a brief background on military deception operations conducted in recent history. These examples will demonstrate for the reader the application of military deception theory into real world situations. There are many examples of operational military deception operations run by both the Allied and Axis powers during World War II, but one of the most exceptional was conducted by the Soviet Union in 1944 in support of Operation Bagration, an offensive against the German forces on the Eastern front. During World War II the Soviets took great advantage of *maskirovka*, which loosely translates as the art of deception.[18] The *maskirovka* efforts put into place for Operation Bagration were the largest and most comprehensive conducted by the Soviets during World War II.[19] In 1944, Soviet intelligence was aware that the Germans knew not only that an

offensive was being prepared, but that they expected the attack to come from the Ukraine towards the Balkans.[20] In Hitler's mind this was the most likely direction of attack because it was the most favorable to the Soviets both in physical attributes and in keeping with the progress that Soviet forces had already made in that part of the region.[21] Instead, the Soviets chose to attack in the most direct route possible, through Belorussia towards Berlin, while capitalizing on the Nazi's belief of an attack from the south to help ensure operational success.[22]

The *maskirovka* plan began with a diversionary attack to the north of Leningrad, followed by feints in Ukraine.[23] At the same time the real offensive forces would be consolidated for an initial attack through Belorussia to be quickly followed by attacks launched from both northern and southern Ukraine.[24] In order to ensure success of Operation Bagration and its *maskirovka* component, the Soviet leadership relied on the means and techniques that are found in present day doctrine. To maintain operational security over the plan, only four individuals were aware of its entirety, and the importance of control over the air and ground in the vicinity of the deception operations was stressed as paramount.[25] False operational orders were sent to the commander of the 3rd Ukranian Front to enforce Hitler's belief that the Soviets were focusing their forces in that region.[26] To add credibility to the false orders that were being transmitted, the Soviets took advantage of the physical means of deception and employed dummy equipment to simulate the concentration of "…eight-nine [*sic*] rifle divisions, reinforced with tanks and artillery…".[27] To further convince the German leadership that this concentration of force was real, technical means were employed by using false radio nets to simulate normal communication between units of this size.[28] Hitler and his military leadership accepted the deceptions put in place by the Soviets and suffered a

devastating defeat which resulted in the loss of 400 kilometers (248.5 miles) of territory to the Soviet army.[29]

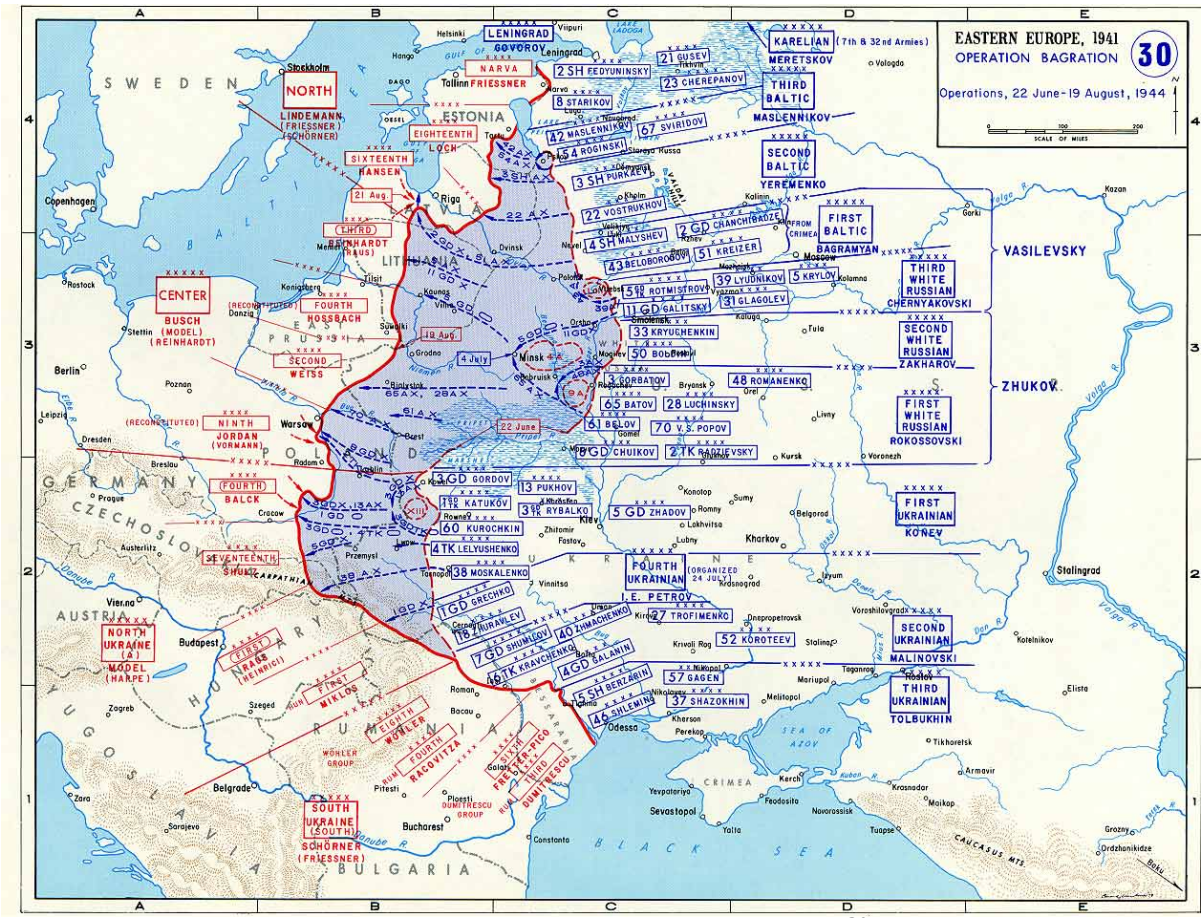

Figure 1. Operation Bagration - 1944[30]

In more recent times deception operations have been acknowledged as having played a significant role in the quick defeat of Iraqi forces that invaded Kuwait in 1990. General Schwarzkopf, Commander in Chief, U.S. Central Command, recognized the importance and utility of deception techniques and included in the coalition plans two major deception operations. The coalition's deception objectives were to promote the appearance of a defensive posture, tie up Iraqi Republican Guard units, and give the appearance that any attack was going to come directly through Kuwait.[31] As noted in the DoD's final report to congress concerning the Persian Gulf War,

> "The first deception enabled the Coalition to achieve tactical surprise at the outset of the air war, even though the attack, given the passage of the United Nations deadline, was in a strategic sense totally expected and predictable. The deception required, for example, the careful planning of air operations during the Desert Shield period, to accustom the Iraqis to intense air activity of certain types, such as refueling operations, along the Saudi border. As a result, the heavy preparatory air activity over Saudi Arabia on the first night of Desert Storm does not appear to have alerted the Iraqis that the attack was imminent."[32]

The report then goes on to describe the second deception operation.

> "The second deception operation confused the Iraqis about the Coalition's plan for the ground offensive. Amphibious landing exercises as well as other activities that would be necessary to prepare for a landing (such as mine sweeping near potential landing areas) were conducted to convince the Iraqis that such an attack was part of the Coalition plan. At the same time, unobserved by the Iraqis who could not conduct aerial reconnaissance because of Coalition air supremacy, the VII Corps and XVIII Airborne Corps shifted hundreds of kilometers to the west from their initial concentration points south of Kuwait. Deceptive radio transmissions made it appear that the two Corps were still in their initial positions, while strict discipline restricted reconnaissance or scouting activity that might have betrayed an interest in the area west of Kuwait through which the actual attack was to be made. The success of this deception operation both pinned down several Iraqi divisions along the Kuwaiti coast and left the Iraqis completely unprepared to meet the Coalition's "left hook" as it swung around the troop concentrations in Kuwait and enveloped them."[33]

As with most historical cases the effectiveness of deception doctrine and its application was proven through the rapid defeat of the Iraqi forces in Kuwait and their forced withdrawal back into Iraq.

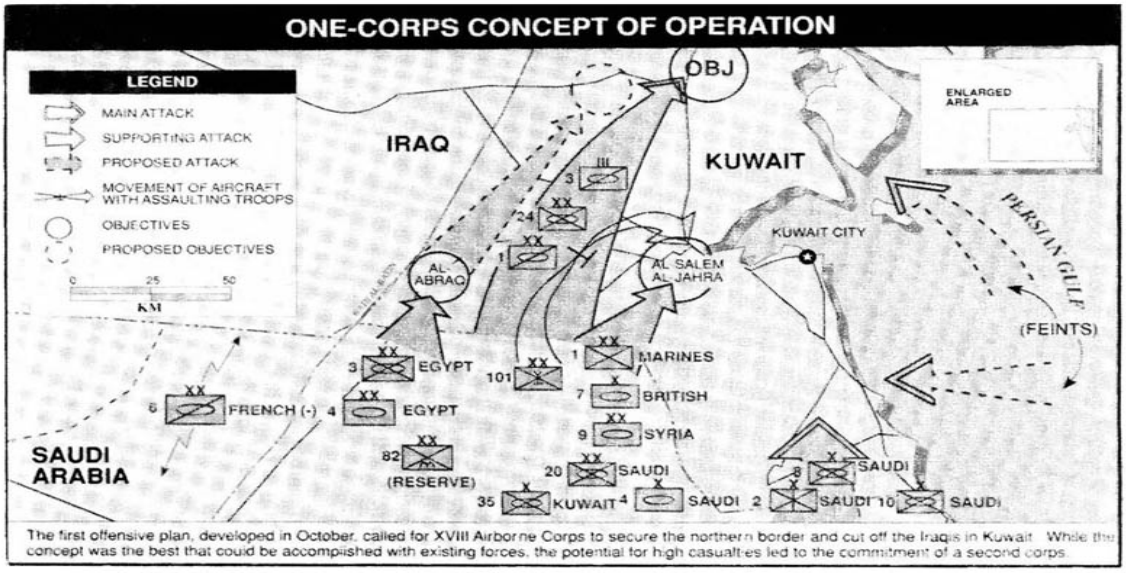

Figure 2. Amphibious feints during Persian Gulf War[34]

INFLUENCING NON-STATE ACTOR DECISION MAKERS

History demonstrates with regularity that military deception doctrine is an effective force multiplier in operations against another state's military force, but can it be applied in the non-state environment? To begin to address this issue, it is necessary to discuss the likely organizational structure of the non-state actor and channels of influence to the leaders of these organizations. There are three general types of organizations used by today's non-state actor: hierarchical based, network based, and a hybrid of the two.[35] A hierarchical organization tends to use a vertical and horizontal command structure, where command relationships are well-defined and there is an orderly information flow.[36] Figure 3 is illustrative of a typical hierarchical organization chart. The hierarchical structure tends to be

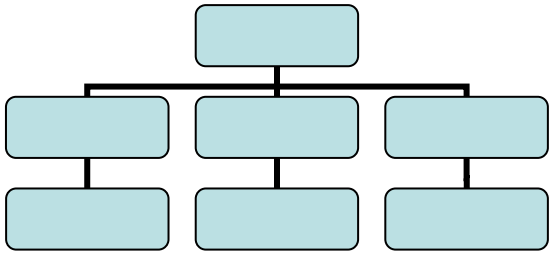

Figure 3. Hierarchical Organization

used by groups that have a more legitimate political wing such as the Chinese Communist Party led by Mao Tse-Tung during its insurgency in the early 1920's and modern day Hezbollah in Lebanon.[37] The hierarchical structure is a benefit to the operational commander since it facilitates identification of the adversary's leadership structure and core decision makers. Another advantage to the hierarchical model is that this is the structure on which the U.S. military is based and is therefore the one which a military deception staff is likely more comfortable confronting. However, the staff must be careful not to assume just because the non-state actor utilizes a hierarchical structure that it necessarily operates in a simple line and block chart manner. Personal relationships within the organization have the potential to

modify the command structure and the flow of information in a way that may not be readily visible to an outside observer.[38]

A networked organization is a more loosely based organization whose objectives require only a limited amount of coordination for their activities.[39] In this model there is not a clear vertical and horizontal command structure, and the flow of information can pass throughout the organization using multiple channels. Typically, organizations that use the network structure have broken their organization into cells that connect to each other in several different fashions. The intent of this type of structure is to limit the direct contact between cells so that if one cell is compromised, the amount of damage to the other cells is minimized. What keeps this type of organization functioning is a binding element consisting of a common belief such as religion or other ideology.[40] There are several types of networked organizations illustrated in figure 4. For the operational commander and his

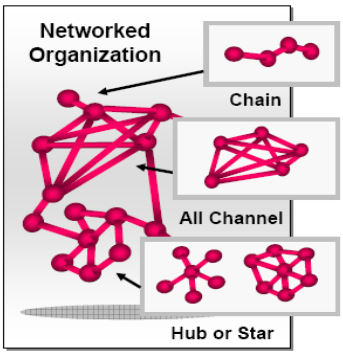

Figure 4. Network Organization Structures[41]

deception planning cell, this is a much more difficult organization to contend with. Depending on the organization, other than the common binding element, there may not be much in the way of formal coordination between the various cells in the network, thus making the identification of leaders of each cell a difficult challenge. Using the current doctrinal model, it will be up to the operational commander to not only identify these leaders

but also to discover ways to influence their decision making process. This means that for each leader who must be influenced, the operational commander is going to have to determine each leader's channel of influence and target each individually. Depending on the size of the non-state actor organization, time may not allow the commander the luxury of completing the process if they are forced to decipher the non-state actor organization on their own. This is why maintaining an intelligence database on such organizations is so important to today's potential battlefield. Ideally, the network organization will already be identified and mapped out for the operational commander, including the key decision makers contained within each cell and the probable methods to influence those individuals.

The hybrid organizational structure utilized by non-state actors is exactly what the name implies, a combination of the hierarchical and network based structures. Al-Qaeda is an excellent example of a hybrid organization. Within Al-Qaeda the senior leadership and core functionaries such as cadre units, are contained within a hierarchical structure. However, in order to accomplish its worldwide objectives, Al-Qaeda utilizes a network structure to maintain a loose affiliation with other terrorist groups who share their Islamic extremist beliefs.[42] For the operational commander the hybrid structure has the advantage of isolating the adversary's decision makers from the rest of the network but makes it more difficult to determine the channels of influence between that leadership and the other non-state actors contained within the network. Again, the best way to combat this difficulty is a continuing intelligence effort that can be relied upon when military deception operations are required.

Once the type of organizational structure is determined and the key decision makers are identified, the operational commander must decide how those leaders can be influenced.

It is through the channels of influence that the commander and his staff have the best chance of conducting a successful deception operation against the adversary. According to Dr. Elena Mastors, a specialist on the psychology of terrorist leaders, there are four main aspects to a leader's framework: personal characteristics, operating environment, advisory process, and information environment.[43] It is within this framework that the operational commander can come to understand his adversary and his associated weaknesses that are open to exploitation by deception.

When looking at a leader's personal characteristics, the idea is to focus "…on the leader's view of self, to include degree of self confidence and locus of control, personal perception of the role they play and how they became leaders, ideology and philosophy, motivation (task, affiliation or power), beliefs, values, proclivities, and likes and dislikes."[44] When these categories are examined, the operational commander should have an idea of what his adversarial leader considers normal to his everyday life, including "…how individuals should behave, impertinent behaviors, words or phrases that can be insulting, and views of the role of minority or majority groups."[45] All of these behaviors can prove insightful as to what information will be acceptable to the adversary and the manner in which the information should be presented.

The leader's operating environment contains the circumstances that brought the individual to power, how his power may be limited by internal or external factors, and the leader's relationship with his internal and external influences.[46] Among these influences the leader's ethnocentric beliefs and outlook on those outside his beliefs must be considered as well.[47] By looking at these elements the operational commander will be able to judge two important factors with regard to deception: core beliefs of the leader and availability of the

leader to outside or differing opinions. In many cases, especially among religiously based non-state actor organizations, the beliefs are likely to be very strongly held and not open to outside influence. This, however, is not necessarily a negative for the operational commander. Instead of fighting the adversary's belief patterns, it may be possible for the commander to reinforce those patterns to take advantage of the potential misconceptions contained within.

The importance of an operational commander's understanding of an adversary's advisory process should be readily apparent. It is often these advisors, both formal and informal, that help to shape the final decisions being made by those in power. Once the individuals who can influence the decision maker are identified, they must be studied in a similar manner as the leader themselves.[48] Included in this study should be "…the potential spin, personal agenda, or filtering of information by [the advisor]…" so that the operational commander can judge his approach to this potential channel of influence.[49] It is also important to remember that advisors may change over time and that there are some leaders who may have advisors but do not heed anyone else's advice but their own.[50]

The last aspect of a leader's personality which should be studied by the operational commander is his adversary's information environment. Most leaders can be broken into complex or simple thinkers.[51] Complex thinkers actively seek out information and operate between the black and white realms of truth in an attempt to understand circumstances as fully as possible.[52] Simple thinkers are more closed to outside information, ignore information that conflicts with their beliefs, and tend to see things in more of a black or white realm of truth.[53] As with the operating environment, while the complex leader offers more avenues of outside influence, the simple leader is an easier target for reinforcing existing

beliefs that are incorrect or contain inaccuracies that are helpful to the operational commander's intentions.

UNCONVENTIONAL HISTORICAL CASE

In 1974 British authorities in Ireland conducted a tactical deception operation against the Irish Republican Army (IRA) which resulted in significantly impacting its operational effectiveness. Following the killing of two constables in Belfast, the British authorities charged five men with the crime, but only two were sent to prison. Both men requested to be housed in the wing of the prison containing members of the IRA. As with all incoming prisoners, the IRA began to question the two men and investigate their background in a typical counter-intelligence fashion. The investigation revealed that both men had been only loosely associated with the IRA and had been removed from the organization for petty crimes. Additionally, it was shown that neither man had committed the crime of which he had been accused. When questioned about these findings both men admitted that they had not committed the crime but insisted that they had been forced to confess by the British. At first both men's stories were accepted at face value, but under further questioning one of the men admitted to being a minor British informant and attempted to implicate his cellmate as well. Slowly the informant began to give information to the IRA, including a list of other individuals within the IRA's organization who were acting as spies for the British. Eventually the informant climaxed his claims with the fact that his confession to the killings was a ruse, and its sole intent was to place him in the prison, giving him access to the IRA leadership within and the ability to kill them with poison that was going to be smuggled in by a prison staff member. These revelations sent the IRA on a witch hunt both within the prison and among its ranks throughout the country. Many individuals implicated by the informant

were summarily killed without an opportunity to counter the charges brought against them. The IRA leadership had also been placed in a position where they did not know whom to trust within their ranks, effectively paralyzing the organization for the next four years. Only later was evidence uncovered showing that the informant had been a British plant from the beginning with the goal of carrying out a deception operation designed to destroy confidence within the IRA's leadership.[54] The British had taken full advantage of the IRA's leadership framework to identify a trait of distrust in others and exploit it though deception to create an ineffective enemy.

CONCLUSION

History has proven that military deception is a useful measure for military commanders confronting a conventional force. In modern times it was successfully implemented throughout World War II and as recently as the Persian Gulf War in 1990. Today's military deception doctrine faces the challenge of adapting itself to an unconventional non-state adversary. Fortunately, deception operations have proven themselves to be adaptable over time and limited in scope only by the bounds of the creativity of the leaders employing them. Military deception operations, depending on the time, space, and force available to the operational commander, may run from the complex to the simple, but all have one goal in mind: to successfully deceive the adversarial leader in a manner that benefits friendly operations. With that in mind it is vital for today's operational commander to spend the time and effort required to understand not only how his enemy thinks but also the operating environment, advisory process, and information environment that influence the decision making process.[55] Intelligence operations must focus on several key factors to enable the commander to make his evaluation of the adversary. Intelligence

must first identify the type of structure under which the non-state actor organization is constructed. This should be followed by identifying the leaders, decision makers, and advisors to these individuals. Once identified, a psychological profile of each individual needs to be constructed, centering on the leadership framework mentioned earlier.[56] It is at this point that the operational commander and his staff will be able to take the clear and complete picture of his adversary, or as clear and complete a picture as possible, and shape current military deception doctrine into an effective tool to achieve victory.

NOTES

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 66.
[2] Mao Tse-Tung, *On Guerrilla Warfare*, trans. Samuel B. Griffith II (Baltimore, MD: The Nautical & Aviation Publishing Company of America, 1992), 73.
[3] Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Washington, DC: CJCS, 13 July 2006), I-1.
[4] Ibid., I-4.
[5] Ibid., I-4.
[6] Chairman, U.S. Joint Chiefs of Staff, *Joint Doctrine for Military Deception*, Joint Publication 3-58 (Washington, DC: CJCS, 31 May 1996), I-1.
[7] Ibid., I-1.
[8] Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Washington, DC: CJCS, 13 July 2006), I-6.
[9] Ibid., I-6.
[10] Ibid., I-6.
[11] Ibid., I-6.
[12] Ibid., I-7.
[13] Ibid., I-7.
[14] Ibid., I-7.
[15] Ibid., I-7.
[16] Ibid., I-7.
[17] Ibid., I-7.
[18] Mark Lloyd, *The Art of Military Deception* (London: Leo Cooper, 1997), 115.
[19] Jon Latimer, *Deception in War* (Woodstock, NY: The Overlook Press, 2001), 250.
[20] Ibid., 250-251.
[21] Ibid., 250.
[22] Ibid., 250-251.
[23] Ibid., 251.
[24] Ibid., 251.
[25] Ibid., 251-253.
[26] Ibid., 252.
[27] Ibid., 252.
[28] Ibid., 252.
[29] Ibid., 250.
[30] United States Military Academy, "Operation Bagration. 22 June – 19 August 1944," http://www.dean.usma.edu/history/web03/atlases/ww2%20europe/WWIIEuropeIndex.html (accessed 16 April 2008).
[31] U.S. Department of Defense, *Conduct of the Persian Gulf War*, Final Report to Congress (Washington, DC: Department of Defense, April 1992), 114 and 124.
[32] Ibid., 34.
[33] Ibid., 34.
[34] Command and General Staff College, "Map 4. One-corps Concept of Operations," http://www-cgsc.army.mil/carl/resources/csi/Swain/swain.asp (accessed 16 April 2008).

[35] U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0) (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007), 3-2.
[36] Ibid., 3-6.
[37] Ibid., 3-2.
[38] Elena Mastors and Jeff Norwitz, *Breaking Al-Qaida* (VA: Potomac Press, forthcoming, 2008).
[39] U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0) (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007), 3-7.
[40] John Arquilla and David Ronfeldt, eds., *Networks and Netwars* (Santa Monica: RAND, 2001), 9.
[41] U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0) (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007), 3-7.
[42] Ibid., 3-2.
[43] Elena Mastors and Jeff Norwitz, *Breaking Al-Qaida* (VA: Potomac Press, forthcoming, 2008).
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] The entirety of this story came from Benjamin I. Higginbotham, *On Deceiving Terrorists*, Research Report no. ADA401353 (Monterey, CA: Naval Post Graduate School, December 2001), 102-105.
[55] Elena Mastors and Jeff Norwitz, *Breaking Al-Qaida* (VA: Potomac Press, forthcoming, 2008).
[56] Ibid.

BIBLIOGRAPHY

Command and General Staff College, "Map 4. One-corps Concept of Operations." http://www-cgsc.army.mil/carl/resources/csi/Swain/swain.asp (accessed 16 April 2008).

Elena Mastors and Jeff Norwitz. *Breaking Al-Qaida*. VA: Potomac Press, forthcoming, 2008.

Higginbotham, Benjamin I. *On Deceiving Terrorists*. Research Report no. ADA401353. Monterey, CA: Naval Postgraduate School, December 2001.

John Arquilla and David Ronfeldt, eds. *Networks and Netwars*. Santa Monica: RAND, 2001.

Latimer, Jon. *Deception in War*. Woodstock, NY: The Overlook Press, 2001.

Lloyd, Mark. *The Art of Military Deception.* London: Leo Cooper, 1997.

Tse-Tung, Mao. *On Guerrilla Warfare*. Translated by Samuel B. Griffith II. Baltimore, MD: The Nautical & Aviation Publishing Company of America, 1992.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1963.

United States Military Academy, "Operation Bagration. 22 June – 19 August 1944." http://www.dean.usma.edu/history/web03/atlases/ww2%20europe/WWIIEuropeIndex.html (accessed 16 April 2008).

U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0). Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007.

U.S. Department of Defense, *Conduct of the Persian Gulf War*. Final Report to Congress. Washington, DC: Department of Defense, April 1992.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Doctrine for Military Deception*. Joint Publication (JP) 3-58. Washington, DC: CJCS, 31 May 1996.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Military Deception.* Joint Publication (JP) 3-13.4. Washington, DC: CJCS, 13 July 2006.

U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0). Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007.

DO NOT ERASE, ESSENTIAL FOR FORMATTING

NOTES

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 66.
[2] Mao Tse-Tung, *On Guerrilla Warfare*, trans. Samuel B. Griffith II (Baltimore, MD: The Nautical & Aviation Publishing Company of America, 1992), 73.
[3] Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Washington, DC: CJCS, 13 July 2006), I-1.
[4] Ibid., I-4.
[5] Ibid., I-4.
[6] Chairman, U.S. Joint Chiefs of Staff, *Joint Doctrine for Military Deception*, Joint Publication 3-58 (Washington, DC: CJCS, 31 May 1996), I-1.
[7] Ibid., I-1.
[8] Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Washington, DC: CJCS, 13 July 2006), I-6.
[9] Ibid., I-6.
[10] Ibid., I-6.
[11] Ibid., I-6.
[12] Ibid., I-7.
[13] Ibid., I-7.
[14] Ibid., I-7.
[15] Ibid., I-7.
[16] Ibid., I-7.
[17] Ibid., I-7.
[18] Mark Lloyd, *The Art of Military Deception* (London: Leo Cooper, 1997), 115.
[19] Jon Latimer, *Deception in War* (Woodstock, NY: The Overlook Press, 2001), 250.
[20] Ibid., 250-251.
[21] Ibid., 250.
[22] Ibid., 250-251.
[23] Ibid., 251.
[24] Ibid., 251.
[25] Ibid., 251-253.
[26] Ibid., 252.
[27] Ibid., 252.
[28] Ibid., 252.
[29] Ibid., 250.
[30] United States Military Academy, "Operation Bagration. 22 June – 19 August 1944," http://www.dean.usma.edu/history/web03/atlases/ww2%20europe/WWIIEuropeIndex.html (accessed 16 April 2008).
[31] U.S. Department of Defense, *Conduct of the Persian Gulf War*, Final Report to Congress (Washington, DC: Department of Defense, April 1992), 114 and 124.
[32] Ibid., 34.
[33] Ibid., 34.
[34] Command and General Staff College, "Map 4. One-corps Concept of Operations," http://www-cgsc.army.mil/carl/resources/csi/Swain/swain.asp (accessed 16 April 2008).
[35] U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0) (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007), 3-2.
[36] Ibid., 3-6.
[37] Ibid., 3-2.
[38] Elena Mastors and Jeff Norwitz, *Breaking Al-Qaida* (VA: Potomac Press, forthcoming, 2008).
[39] U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0) (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007), 3-7.

[40] John Arquilla and David Ronfeldt, eds., *Networks and Netwars* (Santa Monica: RAND, 2001), 9.
[41] U.S. Army Training and Doctrine Command, *A Military Guide to Terrorism in the Twenty-First Century*, U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0) (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, 15 August 2007), 3-7.
[42] Ibid., 3-2.
[43] Elena Mastors and Jeff Norwitz, *Breaking Al-Qaida* (VA: Potomac Press, forthcoming, 2008).
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] The entirety of this story came from Benjamin I. Higginbotham, *On Deceiving Terrorists*, Research Report no. ADA401353 (Monterey, CA: Naval Post Graduate School, December 2001), 102-105.
[55] Elena Mastors and Jeff Norwitz, *Breaking Al-Qaida* (VA: Potomac Press, forthcoming, 2008).
[56] Ibid.